

# VA SOFTWARE ASSURANCE PROGRAM OFFICE

## VA Code Review Process *eLearning Module*

Start >>

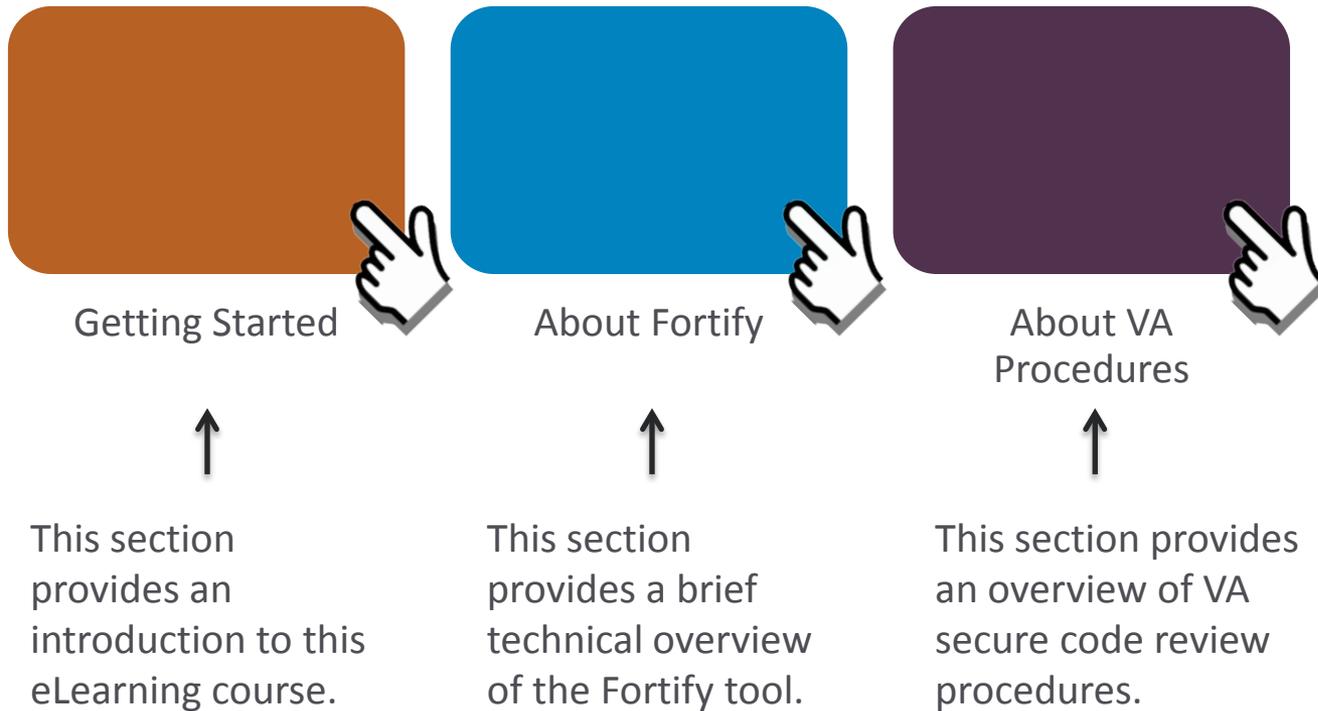


**VA**

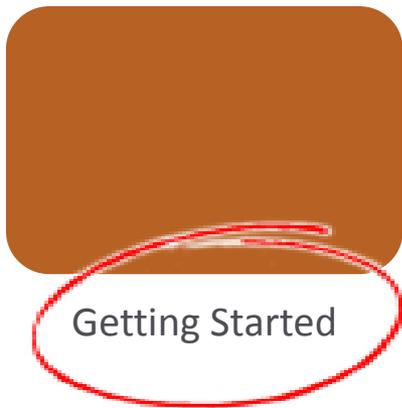


**U.S. Department of Veterans Affairs**  
Office of Information and Technology  
*Office of Information Security*

# VA Code Review Process eLearning Module



# VA Code Review Process eLearning Module



About Fortify

About VA  
Procedures



# Welcome!

1. Welcome

2. Getting Started

3. About Fortify

4. About VA  
Procedures

Thank You

- Thank you for taking the time to review this eLearning module.
- This training module is courtesy of the VA Software Assurance Program Office.
- This training module is an overview of concepts & activities associated with the VA Verification and Validation (V&V) Secure Code Review process.

<< Back

Next >>



# Getting Started...

1. Welcome

2. Getting Started

- What are "V&V Secure Code Reviews"?
- Do I need to do code reviews?
- My ATO / TATO is at the program / system level. How many code reviews are needed?

3. About Fortify

4. About VA Procedures

Thank You

- Reviewing application source code for vulnerabilities can be a complex process.
- The primary objectives of conducting security-focused source code reviews at the VA are to:
  - Improve the security of VA applications agency-wide
  - Encourage the use of static analysis tools during the development of VA applications
  - Ensure that secure code reviews are performed consistently and cost-efficiently

<< Back

Next >>



# What are "V&V Secure Code Reviews"?

1. Welcome
2. Getting Started

- What are "V&V Secure Code Reviews"?

- Do I need to do code reviews?
- My ATO / TATO is at the program / system level. How many code reviews are needed?

3. About Fortify
  4. About VA Procedures
- Thank You

- Generally, VA Application Developers are responsible for performing their own secure code reviews of their applications both during development and the A&A process.
- Secure code review Verification and Validations (V&V) are reviews of developer-performed scans to support obtaining an ATO or TATO that ensure VA requirements for performing secure code reviews have been met.

<< Back

Next >>



# Do I need to do code reviews?

1. Welcome
2. Getting Started
  - What are "V&V Secure Code Reviews"?

- Do I need to do code reviews?
- My ATO / TATO is at the program / system level. How many code reviews are needed?

3. About Fortify
  4. About VA Procedures
- Thank You

- Code reviews are required at the VA under the auspices of the agency-wide Software Assurance program in order to meet FISMA NIST SP 800-53 revision 4 code review requirements that are contained within ProPath.
- ProPath is required for all IT development projects at the VA, agency-wide. ProPath includes System Development Life Cycle (SDLC) activities that have been enhanced by the Software Assurance program to perform code reviews.
- Code reviews are required for all VA software development, with the exception of components that are written in the following languages:
  - MUMPS and
  - Delphi.

<< Back

Next >>



# My ATO / TATO is at the program / system level. How many code reviews do I actually need?

1. Welcome
2. Getting Started
  - What are "V&V Secure Code Reviews"?
  - Do I need to do code reviews?

- My ATO / TATO is at the program / system level. How many code reviews are needed?

3. About Fortify
  4. About VA Procedures
- Thank You

- A code review will need to be conducted for each individual application, and the testing results validated by the Software Assurance Program Office.
- Upon validation, the entire set of code review validation reports will need to be checked into RiskVision in preparation of the A&A process.

<< Back

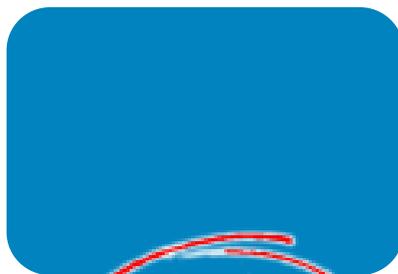
Next >>



# VA Code Review Process eLearning Module



Getting Started



About Fortify



About VA  
Procedures



# About Fortify

1. Welcome

2. Getting Started

3. About Fortify

- What is meant by vulnerabilities in source code?
- How does one search for vulnerabilities in source code using Fortify?
- How does Fortify work?

4. About VA Procedures

Thank You

- What is Fortify?

- The HP Fortify Static Code Analyzer (SCA) tool (a.k.a. Fortify) is a Static Application Security Testing (SAST) tool. This tool can trace through your VA application source code and apply security knowledge to identify vulnerabilities.
- Fortify SCA does not test VA application while it is running or executing, and does not analyze the architecture of the application. It looks only at the source code and requires that the source code can be compiled. As such, all required dependencies must be made available. After a Fortify scan is completed, results are presented in a prioritized fashion, details are provided about each finding reported, including a view of the source code for each finding, along with recommendations of example code fixes or mitigations for each type of finding.

<< Back

Next >>



# What is meant by vulnerabilities in source code?

1. Welcome
2. Getting Started
3. About Fortify

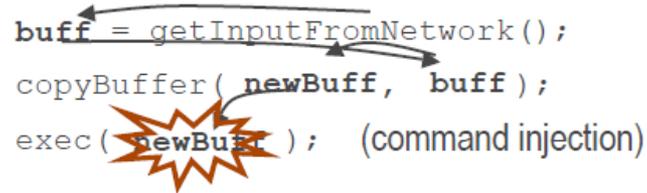
- What is meant by vulnerabilities in source code?

- How does one search for vulnerabilities in source code using Fortify?
- How does Fortify work?

4. About VA Procedures
- Thank You

- Vulnerabilities in source code are flaws in application software implementation and/or design that have security implications.
- Example:

```
buff = getInputFromNetwork();  
copyBuffer( newBuff, buff );  
exec( newBuff ); (command injection)
```



*In this example, external data is read from the network in the `getInputFromNetwork()` function. Note that all external input to the application (not just user input) should be validated prior to use. Fortify checks that the data saved in `buff`, and then copied to `newBuff`, has been validated prior to being used in the `exec()` function call. Fortify will flag this finding as a Command Injection flaw, since no validation occurred. Validating external input should include checking that the data is of a valid type, within an expected range of values, etc.*

*Missing input validation is the #1 cause of many vulnerabilities in application source code. There are many ways to validate data appropriately, depending on how the data is used by the application and how the data values can be constrained.*

<< Back

Next >>



# How does one search for vulnerabilities in source code using Fortify?

1. Welcome

2. Getting Started

3. About Fortify

- What is meant by vulnerabilities in source code?

- How does one search for vulnerabilities in source code using Fortify?

- How does Fortify work?

4. About VA Procedures

Thank You

- Security-focused source code reviews at the VA should be performed using Fortify, which is made freely available by VA to VA application developers, including contractors.
  - Fortify benefits:
    - Fast compared to manual review or security testing
    - Consistent and repeatable
    - Security knowledge built-in
    - Makes security review process easier for non-experts
  - Fortify limitations:
    - Does not understand architecture
    - Does not understand application semantics
    - Does not understand business context

<< Back

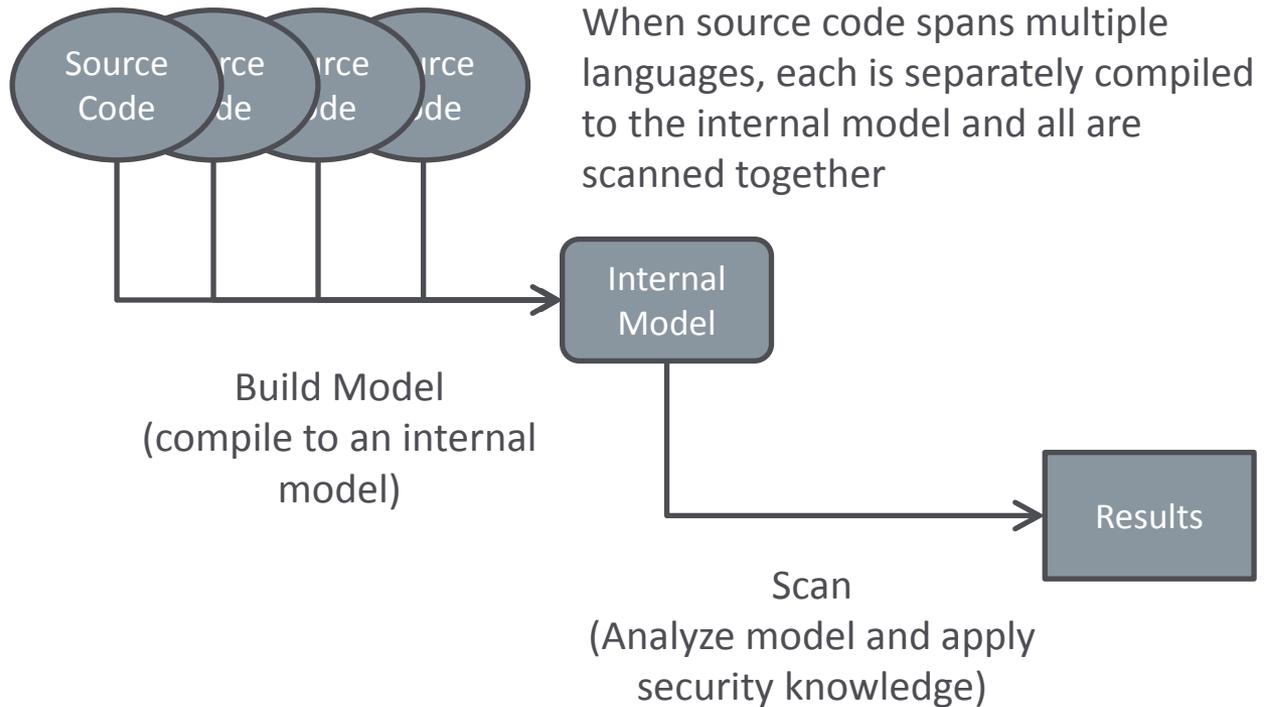


Next >>



# How does Fortify work?

1. Welcome
  2. Getting Started
  3. About Fortify
    - What is meant by vulnerabilities in source code?
    - How does one search for vulnerabilities in source code using Fortify?
    - How does Fortify work?
  4. About VA Procedures
- Thank You



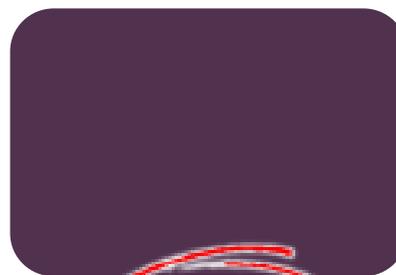
# VA Code Review Process eLearning Module



Getting Started



About Fortify



About VA  
Procedures



# How does the V&V Secure Code Review Validation process work?

1. Welcome
2. Getting Started
3. About Fortify

## 4. About VA Procedures

- Overall workflow
- Auditing scans
- What items are checked for during a V&V secure code review validation?
- How often during development should I use Fortify?
- Where can I find more information?

Thank You

- The overall V&V process works as follows:
  1. VA application developers request the Fortify software, then use it during development (and maintenance)
  2. Prior to release, during the A&A process to obtain an ATO/TATO (or per NSOC direction), developers conduct a final Fortify scan
  3. A V&V secure code review validation request package, containing the final Fortify scan, V&V Request Form, and source code to be delivered, is submitted to the VA Software Assurance Program Office.
  4. The VA Software Assurance Program Office validation process checks that no critical or high findings remain, along with other checks, per the SOP.

<< Back



Next >>



# V&V Secure Code Review Validation process workflow:

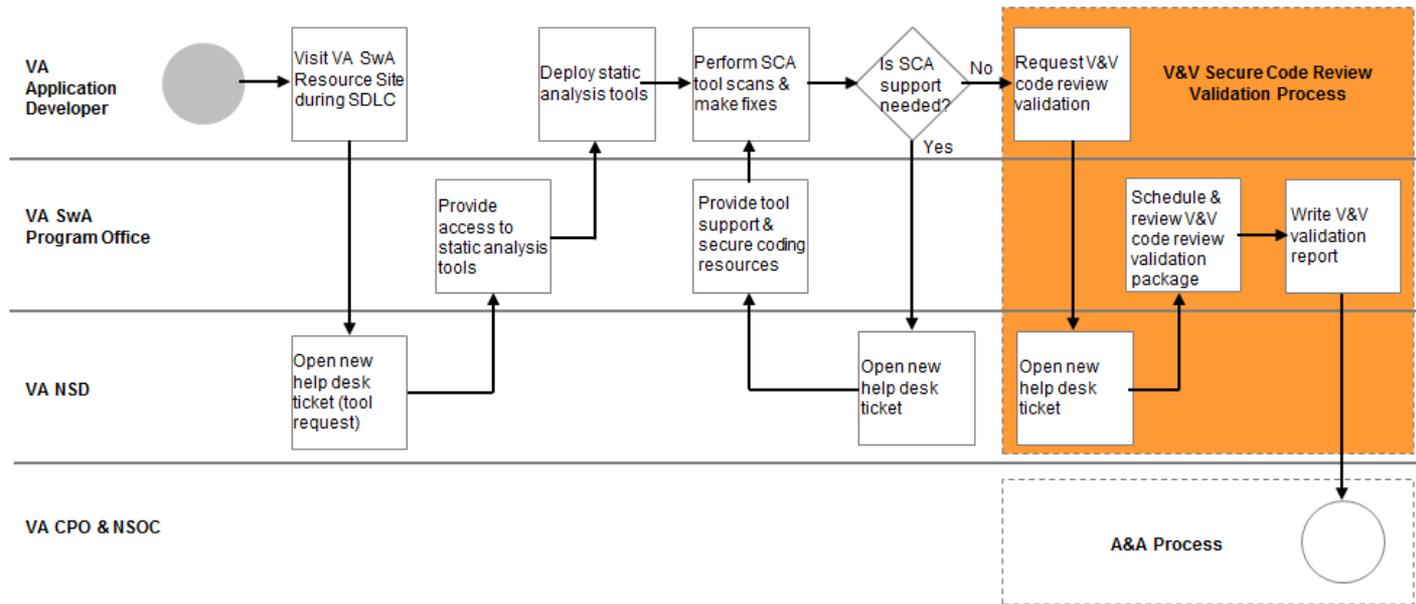
1. Welcome
2. Getting Started
3. About Fortify
4. About VA Procedures

## Overall workflow

- Auditing scans
- What items are checked for during a V&V secure code review validation?
- How often during development should I use Fortify?
- Where can I find more information?

Thank You

- The overall V&V workflow is as follows:



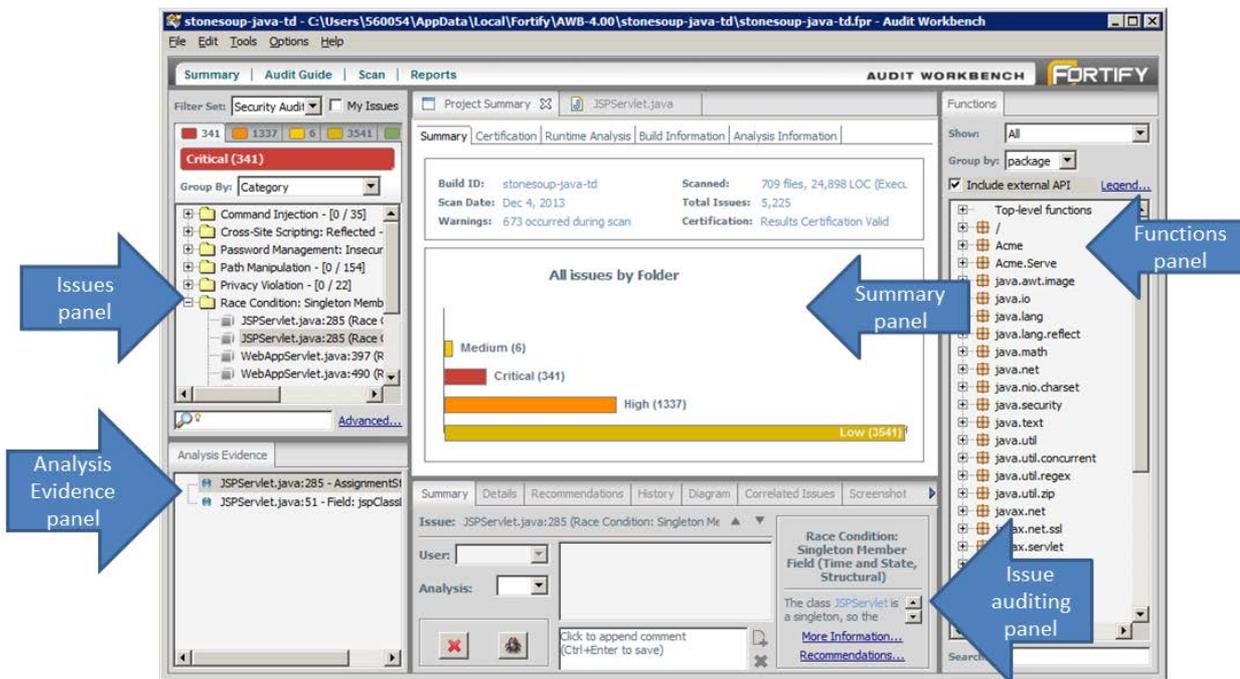
# Auditing Fortify Scans According to VA Procedures

1. Welcome
2. Getting Started
3. About Fortify
4. About VA Procedures

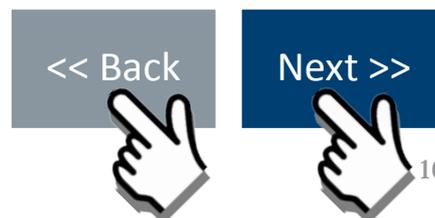
- Overall workflow
- Auditing scans
- What items are checked for during a V&V secure code review validation?
- How often during development should I use Fortify?
- Where can I find more information?

Thank You

- Getting started auditing scan results using Fortify Audit Workbench:



- (Continued on next slide)



# Auditing Fortify Scans According to VA Procedures (Continued)

1. Welcome
2. Getting Started
3. About Fortify
4. About VA Procedures

- Overall workflow
- Auditing scans
- What items are checked for during a V&V secure code review validation?
- How often during development should I use Fortify?
- Where can I find more information?

Thank You

- All findings reported by Fortify need to be audited – Critical, High, Medium, Low

*Tip: Check that the Filter Set drop down box is set to "Security Auditor View." Additionally, do not hide, suppress, or attempt to filter out any issues. All issues reported by Fortify must be viewed and audited.*

- To audit findings, the information provided by Fortify should be reviewed in the Details, Recommendations, and Diagram tab of Audit Workbench. Ensure findings flagged by Fortify are understood.
- Determine if findings require a code fix, are mitigated by other controls in the system, or are a false positive.
- Select the appropriate option from the Analysis pull-down in the Summary tab of Audit Workbench.
- (Continued on next slide)

<< Back

Next >>



# Auditing Fortify Scans According to VA Procedures (Continued)

1. Welcome
2. Getting Started
3. About Fortify
4. About VA Procedures
  - Overall workflow
  - Auditing scans
  - What items are checked for during a V&V secure code review validation?
  - How often during development should I use Fortify?
  - Where can I find more information?

Thank You

- (Continued from previous slide)
- Add comments to the Comments text area to provide details about the other mitigating controls or why an issue is considered a false positive (denoted by selecting “Not an Issue” in the Analysis pull-down).
- Multiple issues can be audited at once by selecting a group of issues and then selecting the appropriate Analysis option and entering comments that apply to all the issues selected
- Fortify provides merge functionality, so the analysis performed on an FPR file can be “merged” with subsequent scans. One only needs to audit the findings once and then merge the audited FPR with future scans of the code base.

<< Back



Next >>



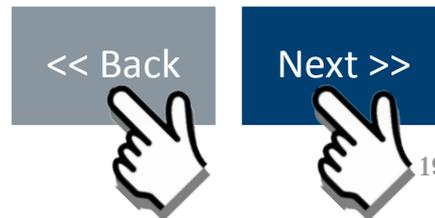
# What items are checked for during a V&V secure code review validation?

1. Welcome
2. Getting Started
3. About Fortify
4. About VA Procedures
  - Overall workflow
  - Auditing scans
  - What items are checked for during a V&V secure code review validation?

Thank You

- Specific items that are checked for include the following:
  - Review developer-provided scan file for matching source code (the source code delivered must match the source code scanned with Fortify)
  - Review developer-provided scan file for scanning issues (Fortify scans must complete successfully, with not errors, exceptions, or warnings reported by Fortify)
  - Review developer-provided scan file for residual findings (all findings reported by Fortify must be audited, with comments added for any issues not fixed, or determined to be “Not an Issue”)
  - Review developer-provided scan file for suppression of issues (all issues reported by Fortify must be visible in the Fortify results)
  - Perform additional supporting analysis, as needed (the SwA team will review the source code and report any additional findings not reported by Fortify, or false negatives)

*Tip: A technical note that provides additional details about steps that need to be performed by developers can be found here:*  
<https://wiki.mobilehealth.va.gov/pages/viewpage.action?pageId=30769185>



# How often during development should I use Fortify?

1. Welcome
2. Getting Started
3. About Fortify
4. About VA Procedures

- Overall workflow
- Auditing scans
- What items are checked for during a V&V secure code review validation?

- How often during development should I use Fortify?

- Where can I find more information?

Thank You

- Generally, Fortify should be used during development as early and as often as possible. The goal should be to identify vulnerabilities early and fix them early. It is far less expensive to find vulnerabilities early in the development process and not let them propagate throughout the source code. When it comes time to do a final scan during the A&A process, there should be minimal issues reported, as a result of all the earlier scans conducted, and the findings fixed.

*Tip: Always check for and use the latest version of the Fortify software and always keep rulepacks up to date. Fortify typically releases a new version of its software 3 or 4 times a year. Rulepacks are generally updated once every couple of months as well. It is recommended that you enable Fortify to automatically check for and download the latest rulepacks every 15 days*

- For projects that use continuous integration, automating Fortify scans as part of your build process may be needed, rather than relying on individual developers to perform scans on their own machines periodically.
- However using Fortify prior to the A&A process is up to developer and respective teams discretion. The SwA team reviews the final scan that is submitted as part of the Secure Code Review Validation package, which is required when attempting to obtain an ATO/TATO. Also see the VA ProPath BLD SDLC requirements.

<< Back

Next >>



# Where do I find the necessary forms, procedures, and help for code reviews?

1. Welcome
2. Getting Started
3. About Fortify
4. About VA Procedures
  - Overall workflow
  - Auditing scans
  - What items are checked for during a V&V secure code review validation?
  - How often during development should I use Fortify?

- Where can I find more information?

Thank You

- The VA Software Assurance Program office provides a support web site that is accessible both inside and outside of the VA network.
  - Link to VA Software Assurance support site :
    - <https://wiki.mobilehealth.va.gov/display/OISSWA>
- The VA Software Assurance Program office provides instructor-led virtual developer training throughout the year:
  - Fortify End User Course (2 Days)
  - Secure Coding Course (3 Days)
- Course schedules and registration information can be found on the home page of the support site in blog announcements.
- Course materials can be freely downloaded in between sessions from the Public Document Library section of the support site.

<< Back



Next >>



# Thank you!

1. Module Selection
2. Getting Started
3. About Fortify
4. About VA Procedures

Thank You

- If you need additional assistance in the future, please contact us for an in-person overview Lync meeting to address any other questions, or project-specific questions :
  - [OISSwASupportGroup@va.gov](mailto:OISSwASupportGroup@va.gov)

<< Back

Reset >>

